(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（A）**　(11)特許出願公開番号

特開平8－106382

(43)公開日　平成８年(1996)４月23日

(51)Int.Cl.[6]	識別記号	庁内整理番号	ＦＩ	技術表示箇所
Ｇ０６Ｆ　9/06	５５０　Ａ	7230－5B		
	Ｋ	7230－5B		
Ｇ０９Ｃ　1/00		7259－5Ｊ		
Ｇ１１Ｂ　19/02	５０１　Ｎ	7525－5D		

審査請求　未請求　請求項の数15　ＯＬ　（全 18 頁）

(21)出願番号　特願平6－225228

(22)出願日　平成６年(1994)９月20日

(31)優先権主張番号　特願平6－219372

(32)優先日　平６(1994)８月10日

(33)優先権主張国　日本（ＪＰ）

(71)出願人　000005223
富士通株式会社
神奈川県川崎市中原区上小田中1015番地

(72)発明者　秋山　良太
神奈川県川崎市中原区上小田中1015番地
富士通株式会社内

(72)発明者　吉岡　誠
神奈川県川崎市中原区上小田中1015番地
富士通株式会社内

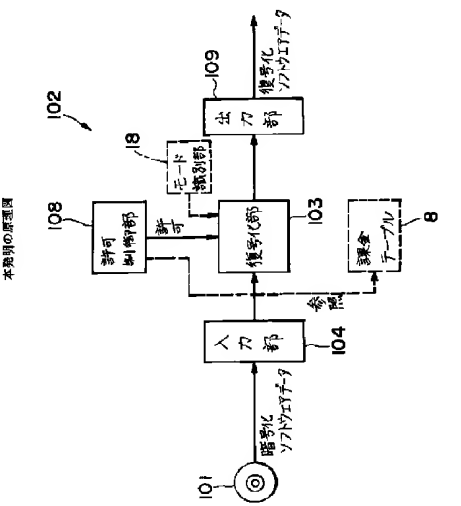
(74)代理人　弁理士　遠山　勉　（外１名）

(54)【発明の名称】　ソフトウエア管理モジュール、ソフトウエア再生管理装置およびソフトウエア再生管理システム

(57)【要約】

【目的】　ソフトウエアの格納媒体を複雑にすることなく、より一層のセキュリティチェックと効率的な課金管理の可能なソフトウエアの管理方式を提供する。

【構成】　ソフトウエア格納媒体や通信から得られる暗号化ソフトウアに対して、ハードウエアに内蔵あるいは着脱可能なソフトウエア管理モジュールを提供し、このソフトウエア管理モジュールには、暗号化されたソフトウエアを復号化する機能を持たせるとともに、許可制御部を設けて復号を許可するか否かを管理するようにした。



1

【特許請求の範囲】

【請求項１】　暗号化された所定のソフトウエア（プログラムおよび／またはデータ）を選択して再生するためのソフトウエア再生装置に装着されるソフトウエア管理モジュールであって、

前記暗号化ソフトウエアを入力する入力部と、

所定の暗号化ソフトウエアの復号を許可する許可制御部と、

前記許可制御部により許可され前記入力部で入力された暗号化ソフトウエアを復号する復号化部と、

前記復号化部で復号された復号化ソフトウエアを出力する出力部とからなるソフトウエア管理モジュール。

【請求項２】　前記に加えて、課金情報記憶部を備えており、前記許可制御部は当該課金情報記憶部を参照してソフトウエア格納媒体からの所定のソフトウエアの復号を許可する請求項１記載のソフトウエア管理モジュール。

【請求項３】　前記に加えて、暗号化部を備えており、前記許可制御部は暗号化ソフトウエアを復号化して得られたプログラムより発生または加工されたユーザ情報を外部に出力する際に当該暗号化部によって当該ユーザ情報を暗号化する請求項１記載のソフトウエア管理モジュール。

【請求項４】　前記ユーザ情報は課金情報である請求項３記載のソフトウエア管理モジュール。

【請求項５】　前記復号化部は、前記暗号化ソフトウエアの特性に応じて復号化の暗号利用モードを変更可能なモード識別部を備えていることを特徴とする請求項１記載のソフトウエア管理モジュール。

【請求項６】　前記復号化部は、入力側に配置された入力用バッファと、

入力データに対して所定の論理による暗号化または復号化を実行する復号化実行部と、　前記復号化実行部の前段に配置された中間レジスタと、

前記入力レジスタと、前記中間レジスタの間に配置され、前記入力レジスタからの出力と復号化実行部からの出力とのいずれかを選択的に前記中間レジスタに出力するセレクタと、

前記復号化実行部の次段に設けられ復号化されたデータを順次出力する出力用バッファとからなる請求項１記載のソフトウエア管理モジュール。

【請求項７】　前記入力用バッファまたは出力用バッファはシフトレジスタである請求項６記載のソフトウエア管理モジュール。

【請求項８】　暗号化された所定のソフトウエアを格納した格納媒体から暗号化ソフトウエアを読み出すドライブ装置と、

前記格納媒体より暗号化ソフトウエアを読み込んで復調する復調手段と、

前記暗号化ソフトウエアを入力する入力部と、所定の暗

2

号化ソフトウエアの復号を許可する許可制御部と、前記許可制御部により許可され前記で入力された暗号化ソフトウエアを復号する復号化部と、前記復号化部で復号された復号化ソフトウエアを出力する出力部とからなるソフトウエア管理モジュールと、

前記管理モジュールから出力された復号化ソフトウエアを出力する出力手段とからなるソフトウエア再生装置。

【請求項９】　前記請求項８において、ソフトウエア管理モジュールを内蔵したカード媒体を装着可能なカードドライブ装置を備えている請求項８記載のソフトウエア再生装置。

【請求項１０】　管理センタとソフトウエア再生装置とからなり、

前記管理センタは、前記ソフトウエア再生装置からの使用要求に対して鍵情報を許諾コマンドとして発行する許諾コマンド発行手段を有しており、

前記ソフトウエア再生装置は、前記鍵情報に基づいて前記ソフトウエアの復号化を実行する復号手段を備えているソフトウエア再生管理システム。

【請求項１１】　前記管理センタは、ユーザの課金情報を蓄積する課金情報蓄積手段を有しており、前記ソフトウエア再生装置が課金情報を前記管理センタに通知する際に当該情報を暗号化する暗号化手段を備えていることを特徴とする請求項１０記載のソフトウエア再生管理システム。

【請求項１２】　前記管理センタは、暗号化または非暗号化ソフトウエアよりチェックサムを生成する送信側チェックサム生成部を有し、

前記ソフトウエア再生装置は、前記管理センタより前記ソフトウエアとチェックサムとを受け取り、当該ソフトウエアよりチェックサムを生成する受信側チェックサム生成部と、この受信側チェックサム生成部で生成されたチェックサムと前記管理センタより受け取ったチェックサムとを比較する比較手段とを有する請求項１０記載のソフトウエア再生管理システム。

【請求項１３】　前記管理センタは、前記ソフトウエアを暗号化する暗号化部を有しており、前記送信側チェックサム生成部は前記暗号化部により暗号化される前のソフトウエアまたは暗号化された後のソフトウエアに対してチェックサムの生成を行うことを特徴とする請求項１２記載のソフトウエア再生管理システム。

【請求項１４】　前記請求項１のソフトウエア管理モジュールにおいて、前記請求項１２の比較手段による比較結果を表示する表示手段を備えているいる請求項１２のソフトウエア再生管理システム。

【請求項１５】　前記比較手段は前記両チェックサムが等しかった場合にのみ課金情報記憶部に対して従量課金を実行する請求項１２記載のソフトウエアの再生管理システム。

【発明の詳細な説明】

【０００１】

【産業上の利用分野】本発明は、コンピュータプログラムあるいは映像著作物等のソフトウエア、特にデジタル情報化されたソフトウエアの流通システムに適用して有効な技術に関する。

【０００２】

【従来の技術】ＣＤ－ＲＯＭ等の大規模記憶媒体や、Ｂ－ＩＳＤＮ等の大容量の高速通信技術などが発達してくると、これらの手段を用いてコンピュータプログラムは勿論、画像や音声をデジタル情報として流通されることが予想される。

【０００３】すなわち、従来ビデオテープで供給されていたような映像著作物がそのままＣＤ－ＲＯＭに格納されて販売されたり、またはＣＤ－ＲＯＭのインタラクティブ性（双方向性）を利用したゲームとして市場に流通し始めてきている。

【０００４】また、通信回線についても同様であり、前記のような映像著作物が通信を経由してユーザの手許に届けられる状況になってきている。ところで、この種のデジタル情報は他の媒体への複写が極めて容易であり、かつアナログ情報のような複写による劣化がないことから、同一情報の複製が可能であり、これらの行為により製造者の利益が害される可能性が極めて高い。すなわち、大容量の書換え可能な光磁気ディスクや磁気ディスク装置さえ所有していればわずかなＤＯＳのコマンドの知識のみでＣＤ－ＲＯＭの内容を複写することが簡単であった。

【０００５】このように、十分なセキュリティチェックが不可能であることを理由にこの種のデジタル情報媒体のレンタル行為は製造者によって禁止されている場合が殆どである。

【０００６】しかしながら、エンドユーザとしては現在のこの種のソフトウエアの価格は高額であり、本当にそのソフトウエアが自身の欲しているものと一致するか、あるいは自身の所有しているハードウエアで使用可能かの確認がとれるまでは購入を躊躇する場合が多い。

【０００７】この点について、機能が制限されている多数のソフトウエアをＣＤ－ＲＯＭに格納して安価に販売し、エンドユーザはその中から希望するソフトウエアについて代金を送金することにより機能制限を解除するコードを通知されるという新しいソフトウエアの流通方式が実現され始めている。

【０００８】

【発明が解決しようとする課題】しかし、前述のソフトウエアの流通方式はソフトウエアの特性を十分に反映したものとはいえなかった。

【０００９】すなわち、前述の機能制限を解除する方式では、代金を一括して送金する場合が殆どであり、この代金はいきおい高額にならざるを得ず、たとえば映画の一場面を少しだけ見たいとか、１週間だけ表計算ソフトを使用したいというような場合にその使用量に応じた料金管理は困難であった。

【００１０】この点について、特公平６－１９７０７号公報では、あらかじめ利用可能金額をＩＣカードに登録し、有償ソフトウエアを利用する場合に前記ＩＣカードの利用可能金額をシステムに登録して、システムが当該ソフトウエアの利用毎に残高を減算していく方式が提唱されている。

【００１１】また、本出願人による特願平６－９６８７１号公報では、ＣＤ－ＲＯＭ等の記憶媒体上に書換え可能領域を設けて使用時間の情報を管理していく方式が提唱されている。

【００１２】本発明は、これらの先行技術をさらに一歩進めたものであり、ソフトウエアの格納媒体を複雑にすることなく、より一層のセキュリティチェックと効率的な課金管理の可能なソフトウエアの管理方式を提案するものである。

【００１３】

【課題を解決するための手段】本発明のソフトウエア管理モジュール１０２は、原理図である図１に示すように、プログラム、文字、図形、画像または音声等からなり暗号化された所定のソフトウエアを選択して再生するためのソフトウエア再生装置に装着され、前記ソフトウエア格納媒体とは別体で構成されたソフトウエア管理モジュールにおいて、前記暗号化ソフトウエアを入力する入力部を設け、所定の暗号化ソフトウエアの復号を許可する許可制御部を設け、前記許可制御部により許可され前記入力部で入力された暗号化ソフトウエアを復号する復号化部をさらに設けるとともに、前記復号化部で復号された復号化ソフトウエアを出力する出力部を設けた。

【００１４】

【作用】前記したように、本発明では、暗号化ソフトウエアを入力する入力部１０４を有している。本発明では、この入力部１０４に入力される暗号化ソフトウエアは、同図に示すＣＤ－ＲＯＭ１０１のような格納媒体からのものであってもよいし、通信回線を通じて得られたデータであってもよい。またデータの種類としては、プログラムは勿論、文字、図形、画像または音声などの如何なる情報であってもよい。

【００１５】入力部１０４の次段には前記暗号化ソフトウエアの復号を行う復号化部１０３が設けられている。この復号化部１０３は、いわゆるＤＥＳ回路（Data Encryption Standard）で構成されており、ＣＰＵ等で構成された許可制御部１０８によって制御されている。

【００１６】また、復号化部１０３は種々の復号モードの中からソフトウエアの特性に応じて最適の復号モードが選択できるよう、モード識別部１８（図３参照）を持たせてもよい。

【００１７】一方、許可制御部１０８は、課金テーブル８（課金情報記憶部）を参照して課金残高がある場合に

のみ復号化部１０３での復号処理を許可するようにしてもよい。この場合、ソフトウエアの再生に応じて課金テーブル８に対して従量課金を実行する。すなわち許可制御部１０８は、課金テーブル８のカウント値を減算していく処理を行う。

【００１８】そして、課金残高が０値となった場合には、出力部１０９に対して課金残高が無くなったことを通知してもよい。これによって出力部１０９は、出力される復号化ソフトウエアに画像データを含む場合には、画面上に課金残高が無くなったことを表示する文章をスーパーインポーズするようにしてもよい。

【００１９】このように、本発明によれば、ソフトウエア再生装置に装着されるモジュール内に許可制御部１０８と、復号化部１０３が設けられているため、セキュリティの高いソフトウエア課金が可能となる。

【００２０】さらに、課金テーブル８もこのモジュール内に収容し、この課金に関する情報（ユーザ情報）を外部に出力する場合には、暗号化部を設けて暗号化することによりセキュリティを高めることができる。この暗号化部は、具体的には前述の復号化部１０３と兼用することができる。

【００２１】さらに、復号化部１０３には、入力用バッファと出力用バッファとを設けてデータの入力と出力とを並列に行わせることにより復号処理を高速化できる。

【００２２】

【実施例】以下に図面に基づいて本発明の実施例を説明する。図１２は本発明が提案する超流通システムにおいてそれぞれの当事者（ベンダ：管理センタ，エンドユーザ：ソフトウエア再生装置，流通チャネル）に要求される技術および役割の概念を示した説明図である。

【００２３】同図において示したようにベンダにおいてはチェックコード挿入や暗号化技術などのコピープロテクションに関する問題が重要となり、エンドユーザにおいてはチェックサムコードの採用によるソフトウエアの完全性保証や高速暗号化技術によるファイル転送・管理が重要となる。一方、流通チャネルにおいては、ソフトウエア販売管理機能が重視されてくる。

【００２４】以上の概念を基に、本発明を具体的に説明する。図２は、本実施例に用いられるソフトウエア再生装置の構成を示す機能ブロック図である。

【００２５】なお、本実施例では説明の便宜のため、入力される暗号化ソフトウエアはＣＤ－ＲＯＭに格納されて提供されたものとするが、通信情報として得られたものであってもよい。

（ソフトウエア再生装置の構成）同図に示す破線で囲んだ部分（ＳＤ回路３）が本発明のソフトウエア管理モジュール１０２である。このソフトウエア管理モジュール１０２は、ソフトウエア再生装置内において、ボードあるいはカード形式で固定的に取付けられたものであってもよいし、ソフトウエア再生装置のカードスロット（たとえばＰＣＭＣＩＡ準拠のカードスロット）内に着脱自在に装着されたＩＣカードであってもよい。

【００２６】同図中、１は復調回路・制御回路であり、ＣＤ－ＲＯＭに格納されているＭＰＥＧ規格の画像・音声情報を復調してデコーダ２に送出する機能を有している。デコーダ２は、エラー訂正およびビットの並び替えを実行して最大２メガバイト／秒（平均１メガバイト／秒）の画像・音声情報（暗号情報）をＳＤ回路３に引き渡す。

【００２７】ソフトウエア管理モジュール１０２、すなわちＳＤ回路３では、Ｉ／Ｏ（５：入力部１０４）を通じて受け取った画像・音声情報（暗号情報）を復号化部１０３としてのＤＥＳ（Data Encryption Standard）７が復号してＩ／Ｏ（６：出力部１０９）を通じてＳＤ回路３外のデマルチプレクサ１３に送出する。デマルチプレクサ１３では、音声データと画像データとを分離して、ＭＰＥＧ処理部（ＭＰＥＧ－２）に出力する。ＭＰＥＧ処理部（ＭＰＥＧ－２）は、データ圧縮されたＭＰＥＧ規格の画像・音声情報を伸長する機能を有しており、音声と画像が分離されて出力される際には、同期制御部（ＶＲＣ）によって画像データと音声データとの同期が調整される。

【００２８】そして、出力先がコンピュータ（ＰＣ）である場合にはＭＰＥＧデータはデジタル情報のまま行い、出力先がＴＶモニタまたはスピーカ等である場合にはＤ／Ａ変換を行った後のアナログ情報として出力する。

【００２９】なお、これらの情報のやりとりは許可制御部としてのソフトウエア再生装置１０５内の制御ＣＰＵ１０とＳＤ回路３内の制御ＣＰＵ４とが分担して行うが、ＳＤ回路３内の制御ＣＰＵ４は制御ＣＰＵ１０で兼用してもよい。

【００３０】本実施例のＤＥＳ７は、FIP'S PUB.製の「46DATA ENCRYPTION STANDARD NIST」を使用し、ＭＰＥＧ処理部は、「ISO/IEC CD 13818'1～3」を使用している。

（ＳＤ回路内の機能）ＳＤ回路３では、制御ＣＰＵ４が許可制御部１０８として機能し、ＣＤ－ＲＯＭ１０１より読み込まれた暗号化ソフトウエアについて、ＤＥＳ７での復号を許可するか否かを判定する。

【００３１】この判定に際して制御ＣＰＵ４は、課金テーブル８を参照し、当該テーブル上に課金残高がある場合にのみＤＥＳ７による復号を実行する。すなわち、課金テーブル８には所定の残高値が登録されており暗号化ソフトウエアの復号処理量または処理時間に応じて課金値が減算されるようになっている。この残高値を更新したい場合には、後述の図７に示すように、カード媒体として提供されているソフトウエア管理モジュール１０２を販売店等に持参し、料金を支払うことにより販売店で課金テーブル８の残高値を増加させることができる。

【００３２】なお、ＳＤ回路３内に課金テーブル８を設けない場合には、当該課金値情報をＦＤ装置１２等に出力して記録しておく必要がある。この場合に課金値情報をユーザが可読な状態でフロッピーディスク等の媒体に登録しておくとセキュリティが維持できない。そこで、当該課金値等情報のユーザ情報を外部に出力する場合には、前記制御ＣＰＵ４はＤＥＳ７で当該課金値情報を暗号化して暗号データとして出力するようになっている。

【００３３】すなわち、課金値情報を外部に出力する場合にはＤＥＳ７は暗号化部として機能することになる。なお、課金値情報の出力先はフロッピーディスクに限らず、図７に示すように通信回線を経由した管理センタ３１であってもよい。

【００３４】一方、制御ＣＰＵ４の課金テーブル８、ＦＤ装置１２または管理センタ３１への課金値情報の参照によって課金値が”０”であることが判明した場合の処理については後述する。（ＤＥＳの詳細）図３は、ＤＥＳ７の概略構成を示している。ＤＥＳ７は同図に示すように、ＤＥＳ実行部１５（制御ＣＰＵ４で実現される）を有しており、入力データ（ＩＮ）を鍵情報１６により復号して出力データ（ＯＵＴ）として出力する機能を有している。

【００３５】本実施例において、ＤＥＳ実行部１５はモード識別部１８を有しており、このモード識別部１８は複数のＤＥＳモードの中からそのデータ形式等により最適なモードを選択してＤＥＳ実行部１５に与える機能を有している。

（ＤＥＳモードの説明）次に前記ＤＥＳモードのうち、代表的なロジックを説明する。

【００３６】図４（ａ）は、ＥＣＢ基本モードであり、ＤＥＳ実行部１５において、６４ビットの鍵情報１６により６４ビットの入力データ列を６４ビットの出力データ列として暗号化（または復号化）するモードである。

【００３７】図４（ｂ）は、ＣＢＣモードを示しており、ＤＥＳ実行部１５において６４ビットの入力データ列を６４ビットの鍵情報１６で暗号化（または復号化）した後、再度これをＤＥＳ実行部１５に帰還入力させる。このようにデータを全て入力し終るまでフィードバックを行い最終結果を出力する方式であり、ファイル等のデータ処理に適している。

【００３８】図４（ｃ）は、ＯＦＢモードを示しており、エラーの生じやすい通信データや、一つの誤りが他に与える影響の大きい音声データ等に適している。図４（ｄ）は、ＣＦＢモードであり、自己同期形のデータに適している。

【００３９】前述のモード識別部１８はモードテーブル２０に格納されたこれらのモードのうちデータ形式等を解析して最適なものを読み出してＤＥＳ実行部１５に送出する。ＤＥＳ実行部１５ではこのようにして選択されたモードに基づいて暗号化・復号化処理を行う。

（ＤＥＳ実行部の高速演算処理化）図５は、ＤＥＳ実行部１５のハードウエア構成を示すブロック図である。

【００４０】同図において、入力側には入力用バッファとして、８ビット構成のレジスタが８個接続されて６４ビットのシフトレジスタ（入力レジスタ２１：ＲＥＧ１）が配置されており、次段にはセレクタｓｅｌが配置されている。当該セレクタｓｅｌは、後述のＤＥＳ処理メイン回路２５からの出力か、前記シフトレジスタ２１からの出力かを選択的に入力できるようになっている。

【００４１】セレクタｓｅｌの次段には８ビット構成のレジスタ２３（ＲＥＧ２）が配置されさらにその次段にはＤＥＳ処理メイン回路２５が配置されている。このＤＥＳ処理メイン回路２５がＤＥＳ実行部１５として機能する。すなわち、ＤＥＳ処理メイン回路２５には、図４で説明した各種のＤＥＳモードがＲＯＭ(Read Only Memory)として登録されており、制御ＣＰＵ４からの指示により最適なＤＥＳモードのロジックを選択して復号処理を行うようになっている。

【００４２】前記ＤＥＳ処理メイン回路２５の出力は前記セレクタｓｅｌと出力用バッファとしての出力レジスタ２４（ＲＥＧ３）に分岐されている。そして出力レジスタ２４（ＲＥＧ３）の出力が暗号化または復号化されたデータとして用いられる。

【００４３】この処理のシーケンスを示したものが図６である。図６において、入力レジスタ２１の出力は、次サイクルの最初のクロックでレジスタ２３からの出力としてＤＥＳ処理される。そして次のクロックで出力レジスタ２４より出力される。この出力レジスタ２４からの出力時間に入力側では入力レジスタ２１より次サイクルの暗号化データの取り込みが行われている。

【００４４】このように、本実施例では入力用バッファとしての入力レジスタ２１と、出力用バッファとしての出力レジスタ２４とを設けたことにより、暗号化データの入力と復号化データの出力とをそれぞれ独立して連続的に行うことができるようになった。そのため、従来のＤＥＳのようにサイクリックに入力と出力とを行う場合に較べて高速な復号化・暗号化処理が可能となった。

（本発明を用いたソフトウエア流通形態の全体像）図７は、本発明によって実現されるソフトウエア流通の全体像を示している。

【００４５】本実施例においてソフトウエアは、出荷センタ（ここでは便宜的に管理センタが出荷センタを兼ねているものとする）より流通経路に出荷されるが、このときの形態は、暗号化したソフトウエアをＣＤ－ＲＯＭに格納した状態であってもよいし、通信路上に出荷してもよいし、あるいは光磁気ディスク等の媒体で出荷してもよい。

【００４６】エンドユーザは販売店２７等に赴き（通信販売でもよい）、ソフトウエアが格納されたソフトウエア格納媒体１０１としてのＣＤ－ＲＯＭを購入してく

る。またこれと同時に、当該ソフトウエアを自身のソフトウエア再生装置１０５で再生可能なようにドライバソフト等の運用アプリケーションディスク２６およびソフトウエア管理モジュール１０２であるＳＤカードを購入してくる。ここで、運用アプリケーションディスク２６はたとえばフロッピーディスクの形態であり、これを外部ユーザ情報格納媒体１０６として用いてもよい。また、ＣＤ－ＲＯＭは複数のソフトウエアが格納されているものの、このＣＤ－ＲＯＭを売り切る販売方式ではないため、ＣＤ－ＲＯＭ自体の販売価格は非常に安価に設定されている。また販売店２７はレンタル店であってもよい。

【００４７】すなわち、本発明ではＣＤ－ＲＯＭに格納されたソフトウエアは全て暗号化されており、これを復号して再生する場合にはセキュリティの高く保持されたソフトウエア管理モジュール１０２としてのＳＤカードを用いることが必須である。そして後述のようにソフトウエアの使用量に応じた料金徴収システムが完備されている。したがって、ＣＤ－ＲＯＭ自体に格納されている暗号化データを他の媒体に複写したとしてもそれだけでは意味がなく、ＣＤ－ＲＯＭをレンタル方式としても使用量に対応した料金徴収システムが完備されていればソフトウエア提供者の利益を低下させてしまうことはない。

【００４８】エンドユーザは、自己のソフトウエア再生装置１０５で当該ＣＤ－ＲＯＭ（１０１）に格納されたソフトウエアの再生を望む場合には、まずＳＤカード（１０２）をカードドライブ装置２８に挿入し、ＣＤ－ＲＯＭ（１０１）と運用アプリケーションディスク２６ソフトウエア再生装置１０５にそれぞれ装填する。

【００４９】そして、ソフトウエア再生装置１０５にインストールされた通信アプリケーション（このアプリケーションは運用アプリケーションとして提供されるものでもよい）を起動して、ソフトウエア再生装置１０５に内蔵されたモデム（変調装置）より家庭用電話機３０を通じて管理センタ３１に対して使用したいソフトウエアの使用要求を発信する。これに対して管理センタ３１は、当該ユーザに対して許諾コマンド（鍵情報）を暗号化してソフトウエア再生装置１０５に対して送出する。

【００５０】前記許諾コマンドを受け取ったソフトウエア再生装置１０５は、ＣＤ－ＲＯＭ１０１を読み取り、必要なソフトウエアをＳＤカードの復号部１０３を通じて順次復号化してソフトウエア再生装置１０５のプログラム格納エリア（メモリ）に転送する。

【００５１】これとともに、制御ＣＰＵ４は当該ソフトウエアの復号データ量、または復号時間をカウントし、課金テーブル８より課金残高値を減算する。そしてこの課金残高値が”０”になるまでは暗号化ソフトウエアの復号処理を継続する。

【００５２】ここで、課金テーブルの課金残高値が”０”となった場合には、復号化ソフトウエアの出力を停止する。この出力停止を具体化するハードウエア構成を図８に示している。

【００５３】すなわち、同図では、課金テーブル８を監視していた制御ＣＰＵ３は、課金テーブル上の課金残高値が”０”となったことを検出したとき、この情報をソフトウエア再生装置１０５内の制御ＣＰＵ１０に通知する。この通知に基づいて制御ＣＰＵ１０はレジスタ８１の保持値を変化させて、ＴＶモニタへの出力およびコンピュータ（ＰＣ）への出力段にある論理積回路（ＡＮＤ８３）とアナログスイッチ（ＳＷ８２）を閉じる。これによって出力装置へはアナログ変換された音声情報しか出力されない。

【００５４】なお、これとともに画像出力として課金残高が”０”となった旨の表示あるいは広告等をスーパーインポーズしてもよい。以上の説明は課金残高をＳＤ回路３内の課金テーブル８が管理している場合の例であるが、この課金値残高情報は管理センタ３１が管理していてもよい。この場合、課金値残高情報がソフトウエア再生装置１０５の外部に出力されることになるので、セキュリティを高めるために前述の制御ＣＰＵ３は、ＤＥＳ７を用いて課金値残高情報を暗号化して、暗号化データとして電話回線を通じて管理センタ３１に通知する。

【００５５】管理センタ３１ではソフトウエア再生装置１０５から受領した課金値残高情報にしたがって、金融機関３２のエンドユーザの口座よりエンドユーザが使用した使用量に応じた料金を引き落として当該ソフトウエア提供者の口座に送金する処理を行う。

【００５６】このように、本発明ではＣＤ－ＲＯＭに格納されたソフトウエアばかりでなく、そのソフトウエアの運用によって生じたユーザ情報も暗号化して外部に出力するため、ユーザ情報の改ざんによるソフトウエアの不正使用も防止することができる。

（出荷されたソフトウエアの完全性保証について）ところで、ソフトウエアの流通経路においてソフトウエアにウィルス等が混入され、エンドユーザはウィルスが混入されたソフトウエアを再生することにより、ハードウエアや自己の蓄積したソフトウエアを破壊されたり、さらにはウィルのために正常に動作しないソフトウエアに対しても課金されるおそれが生じてくる。

【００５７】このような流通経路におけるウィルス混入をソフトウエア再生装置１０５において確実に検出できるようにした構成が図９である。すなわち、管理センタ３１にはチェックサム生成部１１１ａが設けられている。このチェックサム生成部１１１ａは出荷すべきソフトウエアからチェックサム（ＣＳ）、すなわちデータの完全性をチェックするコードを生成する機能を有しており、本実施例ではハッシュ関数による関数コードがチェックサム（ＣＳ）として出力されるようになっている。

【００５８】このチェックサム生成部１１１ａのロジッ

クを示したものが図１１である。すなわちここでＤＥＳ暗号による操作を行う場合、基本的にはＣＢＣモード（図４（ｂ）で説明したもの）を構成しており、プログラムあるいはデータを１ブロック単位に区切り、ＣＢＣモード（ブロック帰還）で一旦出力したデータをそのまま帰還入力し、次の入力ブロックとで排他論理和制御（ＥＯＲ）を行う。この結果を再びＤＥＳ暗号化処理して前記と同様に出力を入力側に帰還させる。そして最終ブロックが入力された場合、変換された暗号化出力をチェックサム（ＣＳ）とする。

【００５９】図１０は、ソースプログラムをコンパイラによりオブジェクト化した後、圧縮処理を施しこの圧縮平文オブジェクトプログラムをハッシュ関数ｈに入力して（チェックサム生成部１１１ａで処理して）、チェックサム（ＣＳ）を得、これを前記圧縮平文オブジェクトプログラムに結合する様子を示している。

【００６０】このような暗号化プログラムが流通経路を流通した段階でコンピュータウィルスが混入された場合、ソフトウエア再生装置１０５における下記の機構を用いることによりウィルス混入の確認が容易となる。

【００６１】すなわち、ソフトウエア再生装置１０５には、前記チェックサム生成部１１１ａと同様のチェックサム生成部１１１ｂを有しており、ソフトウエアより前記と同様の方法でチェックサム（ＣＳ’）を生成する。そして、比較部１１２において前記ソフトウエアに添付されてきたチェックサム（ＣＳ）と前記チェックサム生成部１１１ｂで新たに生成されたチェックサム（ＣＳ’）とを比較する。

【００６２】このとき、流通経路上でソフトウエアにウィルスが混入し、ソフトウエアの改変が行われると、チェックサム生成部１１１ｂで生成されるチェックサム（ＣＳ’）は必然的に元のチェックサム（ＣＳ）とは異なる。

【００６３】このように比較部１１２が比較結果に異常を検出したときには表示部１１３において異常を示す赤色表示を行う。この表示はたとえばカード形状で構成されたソフトウエア管理モジュールの一端にスイッチ（ＳＷ）によりその表示状態を変更可能な表示ランプを設けることにより容易に実現できる。また、チェックサム生成部１１１ｂが処理を行っている間は処理中である黄色表示を行い、比較結果が等しく正常終了した場合には青色表示を行うようにした。

【００６４】そして、比較部１１２での比較処理が正常終了した場合にのみ課金テーブル８から従量課金を実行する。具体的には許可制御部１０８（図９では図示省略）が課金テーブル８のカウント値を減算していく処理を行う。

【００６５】図９および図１０で説明したチェックサム生成と、暗号化との関係についてさらに詳しい具体例で示したものが図１３～図２２である。これらの図ではソフトウエアはＣＤ－ＲＯＭに格納されて情報提供者（管理センタ）からエンドユーザ（ソフトウエア再生装置）に供給される場合を想定している。

【００６６】図１３は、平文のソフトウエアから鍵情報（Ｋ１）を用いてチェックサム（ＣＳ）を生成し、これをＣＤ－ＲＯＭの所定領域に格納している。そして、前記平文ソフトウエアは鍵情報（Ｋ２）を用いて暗号化してＣＤ－ＲＯＭ上の前記チェックサム（ＣＳ）の格納された領域以外の領域に格納し、これをエンドユーザに提供する。エンドユーザは、ヘッダ解析を行いながら暗号化ソフトウエアを鍵情報（Ｋ２）で復号しこれを一旦メモリまたはそれ以外の記憶手段に蓄える。そして、復号化された平文ソフトウエアから鍵情報（Ｋ１）を用いてチェックサムを生成し、これをＣＤ－ＲＯＭから読み出されたチェックサムと比較する。そして、比較結果が一致した場合にのみ課金処理を実行する。

【００６７】図１４は、図１３の例において、情報提供者（管理センタ）において暗号化処理を行わない場合である。図１５は、暗号化された情報（ソフトウエア）からチェックサムを生成する点が特徴である。すなわち、平文ソフトウエアを鍵情報（Ｋ２）でまず暗号化してこれをＣＤ－ＲＯＭに格納する。そして暗号化ソフトウエアに対してチェックサムを生成しこれを所定の領域に格納しエンドユーザに供給する。

【００６８】エンドユーザ側ではヘッダ解析を行いながら暗号化ソフトウエアから直接チェックサムを生成し、このチェックサムをＣＤ－ＲＯＭに格納されていたチェックダムと比較する。

【００６９】図１６は、情報提供者（管理センタ）側の処理は図１３と同様であるが、エンドユーザ側（ソフトウエア再生装置側）の課金処理が異なっている。すなわち、ヘッダ解析の結果課金処理を開始するが、チェックサムの比較結果が一致しなかった場合には課金処理を無効（旧状態復帰書換）にするようになっている。

【００７０】図１７は、情報提供者（管理センタ）側の処理は図１４と同様であるが、エンドユーザ側（ソフトウエア再生装置側）の課金処理が異なっている。すなわち、ヘッダ解析の結果課金処理を開始するが、チェックサムの比較結果が一致しなかった場合には課金処理を無効（旧状態復帰書換）にするようになっている。

【００７１】図１８は、情報提供者（管理センタ）側の処理は図１５と同様であるが、エンドユーザ側（ソフトウエア再生装置側）の課金処理が異なっている。すなわち、比較結果に基づいて課金処理を実行しこの課金処理によって復号を開始するようになっている。

【００７２】図１９は、情報提供者（管理センタ）側の処理は図１６と同様であるが、エンドユーザ側（ソフトウエア再生装置側）の課金処理が異なっている。すなわち、ヘッダ解析の結果課金処理を開始するが、チェックサムの比較結果が一致しなかった場合には課金処理を無

効（旧状態復帰書換）にするようになっている。

【００７３】図２０は、情報提供者（管理センタ）側の処理は図１５と同様であるが、エンドユーザ側（ソフトウエア再生装置側）の課金処理が異なっている。すなわち、ヘッダ解析の結果課金処理を開始するが、チェックサムの比較結果が一致しなかった場合には課金処理を無効（旧状態復帰書換）にするようになっている。

【００７４】図２１は、平文ソフトウエアを鍵情報（Ｋ）で暗号化するとともに特定の領域ｎに暗号化データの一部Ｎに対応した情報を登録しておき、エンドユーザ側（ソフトウエア再生装置）で前記Ｎを復号し、これをｎと比較するものである。そして比較の結果が一致すれば課金処理を行うようになっている。

【００７５】図２２は、情報提供者（管理センタ）側の処理は図２１と同様であるが、ヘッダ解析とともに課金処理を開始し、比較結果が一致しなかった場合には課金処理を無効（旧状態復帰書換）にするようになっている。

【００７６】以上説明したように、図９～図２２に示した例では、データの完全性保証の確認が容易であるため、ウィルスが混入されたソフトウエアを再生することにより生じるハードウエアあるいはデータの破壊、不合理な課金を未然に防止できる。

（管理センタによるソフトウエアの貸出時刻管理）次に管理センタ３１によりソフトウエアの利用時刻管理が行われる場合について説明する。

【００７７】前記管理センタ３１はソフトウエア再生装置１０５に対して許諾コマンドを発行するとともに、コンテンツに対応する利用開始時刻（タイムスタンプ）を暗号化して通信回線を通じて（モデム経由でも可）ソフトウエア再生装置１０５に送出する。

【００７８】ソフトウエア再生装置１０５では、このタイムスタンプを受け取ると自身のＳＤ回路３でこのタイムスタンプを復号し、課金テーブル８に書き込む。このときコンテンツ毎に課金テーブル８が設定されているときには該当欄にタイムスタンプを書き込むようにする。

このように、タイムスタンプを管理することによりエンドユーザのソフトウエアの利用期限を管理することができる。

【００７９】なお、暗号化タイムスタンプの配送は、管理センタ３１のオペレータがエンドユーザに対して口頭で伝え、エンドユーザがこれをキーボード等を通じて自身のソフトウエア再生装置１０５に入力するようにしてもよい。このようにしてもタイムスタンプは暗号化されているため、セキュリティは保持できる。

【００８０】なお、以上説明した実施例において、ソフトウエア再生装置１０５へのソフトウエアの提供は、ＣＤ－ＲＯＭのような有形媒体のみに限らず、高速化された通信システムを経由してホストコンピュータより通信データとして得られたソフトウエアであってもよいことは勿論である。

【００８１】

【発明の効果】本発明によれば、ソフトウエアの格納媒体を複雑にすることなく、より一層のセキュリティチェックと効率的な課金管理の可能なソフトウエアの管理を行うことができる。

【図面の簡単な説明】

【図１】　本発明の原理図

【図２】　本実施例のソフトウエア再生装置を示す機能ブロック図

【図３】　本実施例のＤＥＳの内部機能を示すブロック図

【図４】　ＤＥＳの各モードを示す説明図

【図５】　ＤＥＳ実行部のハードウエア構成を示すブロック図

【図６】　ＤＥＳ実行部の処理シーケンスを示す説明図

【図７】　本発明のソフトウエア流通システムの全体概念を示す説明図

【図８】　実施例において、課金テーブルの残高によって出力を停止するためのハードウエア構成図

【図９】　実施例において再生されるソフトウエアの完全性保証を確認するための機構を示すブロック図

【図１０】　実施例において再生されるソフトウエアの完全性保証を確認するためのデータの構成を示すブロック図

【図１１】　実施例におけるチェックサム生成部の機能を示すブロック図

【図１２】　本発明においてそれぞれの当事者に要求される技術、役割の概念を示した説明図

【図１３】　管理センタとソフトウエア再生装置との間で、暗号化またはチェックサムの分担を示すブロック図

【図１４】　管理センタとソフトウエア再生装置との間で、暗号化またはチェックサムの分担を示すブロック図

【図１５】　管理センタとソフトウエア再生装置との間で、暗号化またはチェックサムの分担を示すブロック図

【図１６】　管理センタとソフトウエア再生装置との間で、暗号化またはチェックサムの分担を示すブロック図

【図１７】　管理センタとソフトウエア再生装置との間で、暗号化またはチェックサムの分担を示すブロック図

【図１８】　管理センタとソフトウエア再生装置との間で、暗号化またはチェックサムの分担を示すブロック図

【図１９】　管理センタとソフトウエア再生装置との間で、暗号化またはチェックサムの分担を示すブロック図

【図２０】　管理センタとソフトウエア再生装置との間で、暗号化またはチェックサムの分担を示すブロック図

【図２１】　管理センタとソフトウエア再生装置との間で、暗号化またはチェックサムの分担を示すブロック図

【図２２】　管理センタとソフトウエア再生装置との間で、暗号化またはチェックサムの分担を示すブロック図

【符号の説明】

15

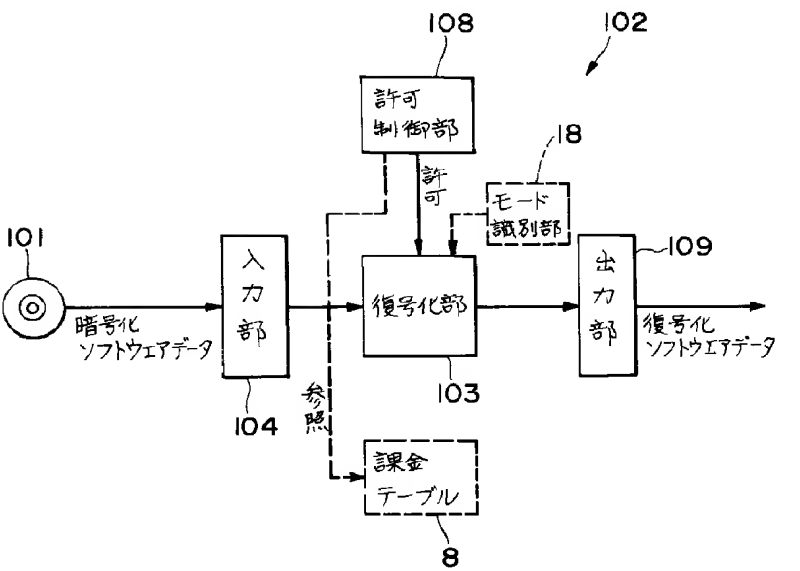
１・・・復調回路・制御回路、
２・・・デコーダ、
３・・・ＳＤ回路、
４・・・制御ＣＰＵ、
５・・・インターフェース（Ｉ／Ｏ）、
６・・・インターフェース（Ｉ／Ｏ）、
７・・・ＤＥＳ
８・・・課金テーブル、
１０・・・制御ＣＰＵ、
１１・・・インターフェース、
１２・・・フロッピーディスク装置、
１３・・・デマルチプレクサ、
１５・・・ＤＥＳ実行部、
１６・・・鍵情報、
１８・・・モード識別部、
２０・・・モードテーブル、
２１・・・入力レジスタ、
２３・・・レジスタ、
２４・・・出力レジスタ、
２５・・・ＤＥＳ処理メイン回路、

16

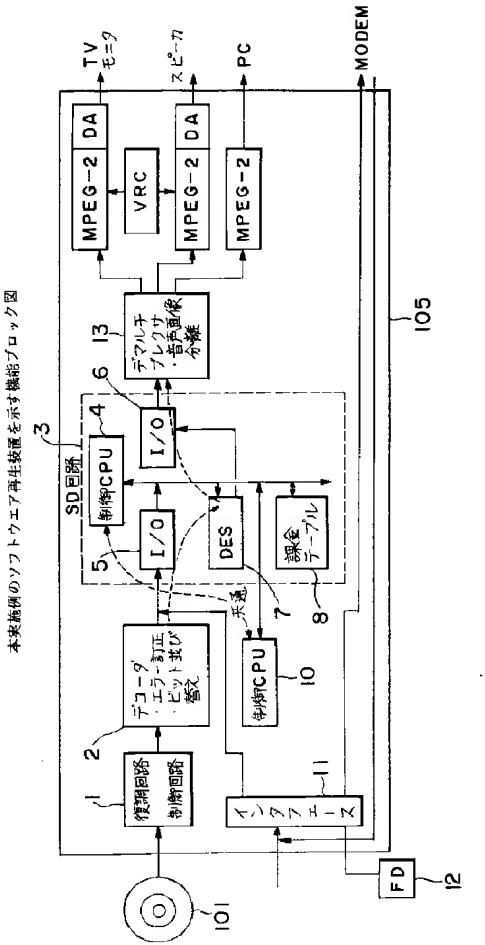
２６・・・運用アプリケーションディスク、
２７・・・販売店、
２８・・・カードドライブ装置、
３０・・・家庭用電話機、
３１・・・管理センタ、
３２・・・金融機関、
１０１・・・ソフトウエア格納媒体、
１０２・・・ソフトウエア管理モジュール、
１０３・・・復号化部、
１０５・・・ソフトウエア再生装置、
１０６・・・外部ユーザ情報格納媒体、
１０７・・・メモリ、
１０８・・・許可制御部、
１１１ａ，１１１ｂ・・・チェックサム生成部
１１２・・・比較部
１１３・・・表示部
ＤＢ・・・データベース、
ＮＴ・・・ネットワーク、
ｓｅｌ・・・セレクタ、

【図１】

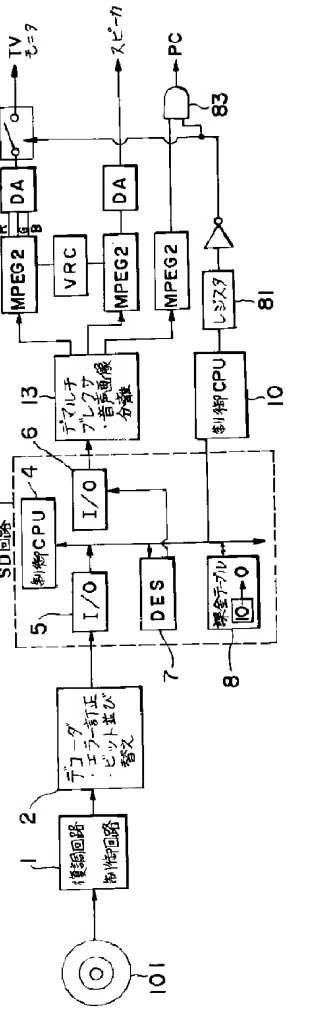
本発明の原理図



【図2】

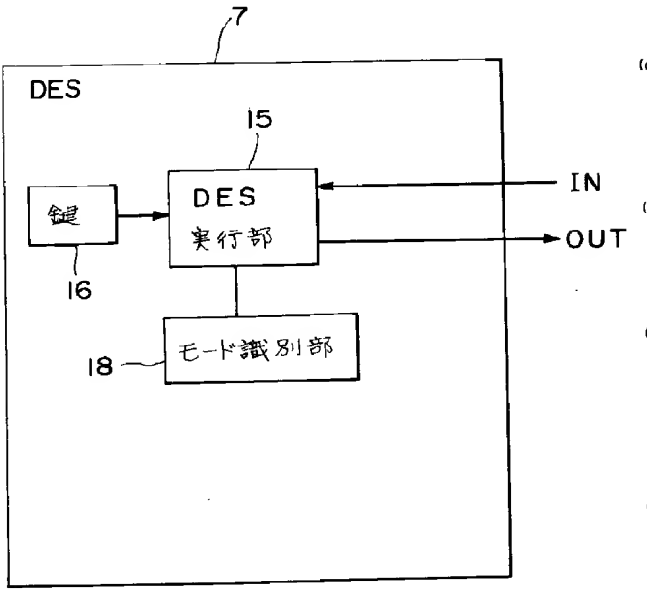

本実施例のソフトウエア再生装置を示す機能ブロック図
TV
モニタ
スピーカ
PC
MODEM
MPEG-2
DA
VRC
デマルチ
ブレクサ
音声画像
分離
SD回路
制御CPU
I/O
DES
課金
テーブル
デコーダ
エラー訂正
ビット並び
替え
制御回路
インタフェース
FD
光通
105
101
12
11
10
8
7
6
5
4
3
2
1
13

【図8】


実施例において、課金テーブルの設定によって出力を停止するためのハードウエア構成図
TV
モニタ
スピーカ
PC
SW
MPEG2
DA
VRC
デマルチ
ブレクサ
音声画像
分離
SD回路
制御CPU
I/O
DES
課金
テーブル
デコーダ
エラー訂正
ビット並び
替え
制御回路
レジスタ
101
81
82
83
10
8
7
6
5
4
3
2
1
13

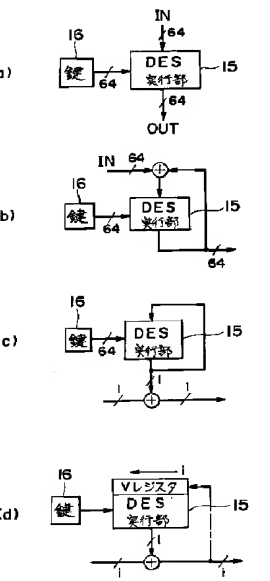
【図３】

本実施例のＤＥＳの内部機能を示すブロック図



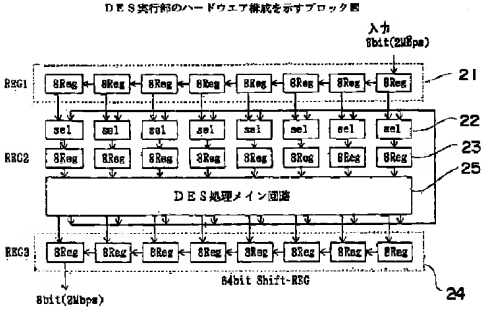
【図４】

ＤＥＳの各モードを示す説明図



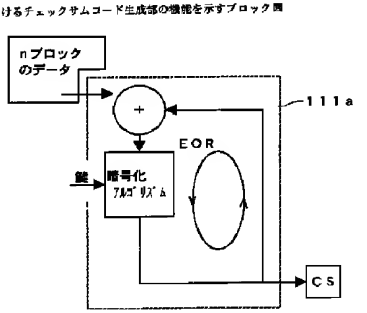
【図５】

ＤＥＳ実行部のハードウエア構成を示すブロック図

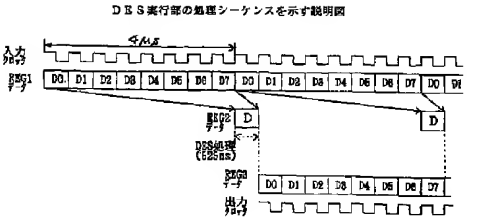


【図１１】

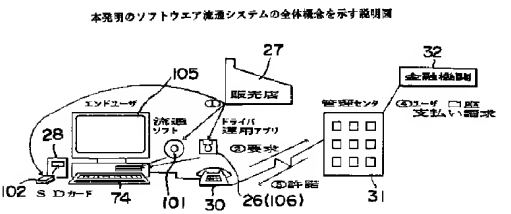
実施例におけるチェックサムコード生成部の機能を示すブロック図



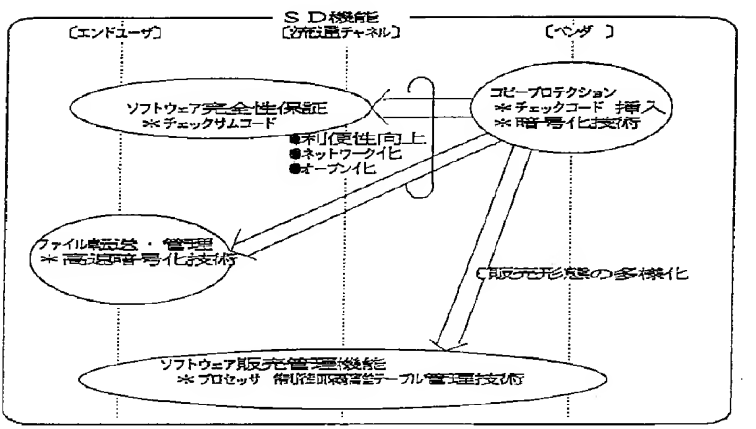
【図６】


ＤＥＳ実行部の処理シーケンスを示す説明図
入力データ
出力データ
D0 D1 D2 D3 D4 D5 D6 D7 D0 D1 D2 D3 D4 D5 D6 D7 D0 D1
D
D
D0 D1 D2 D3 D4 D5 D6 D7

【図７】

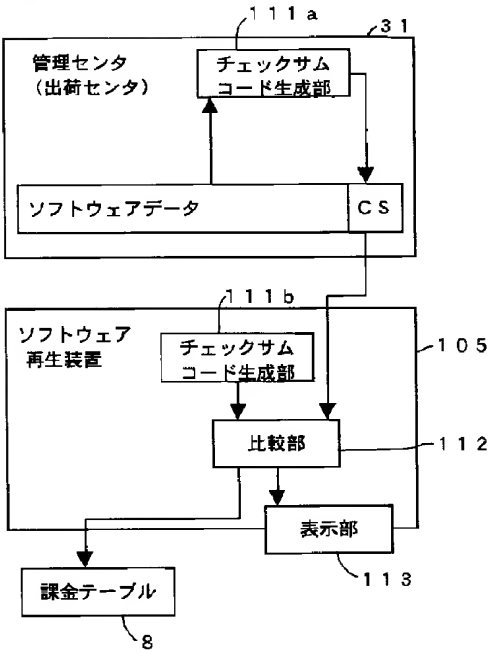

本発明のソフトウエア流通システムの全体概念を示す説明図
27
32
105
販売店
エンドユーザ
流通ソフト
ドライバ運用アプリ
管理センタ
28
102
ＳＤカード
74
101
30
26(106)
31

【図１２】

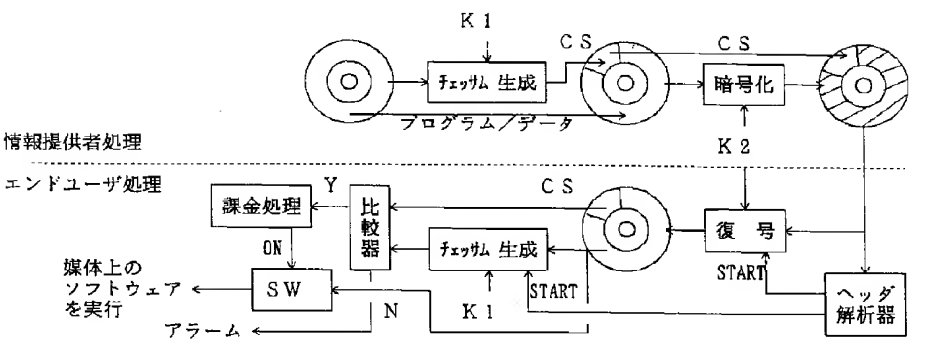

ＳＤ機能
〔エンドユーザ〕
〔流通チャネル〕
〔ベンダ〕
ソフトウェア完全性保証
＊チェックサムコード
コピープロテクション
＊チェックコード 挿入
＊暗号化技術
●利便性向上
●ネットワーク化
●オープン化
ファイル転送・管理
＊高速暗号化技術
販売形態の多様化
ソフトウェア販売管理機能
＊プロセッサ 制御性向上管理テーブル管理技術

【図９】

実施例において再生されるソフトウエアデータの完全性保証を確認するための機構を示すブロック図

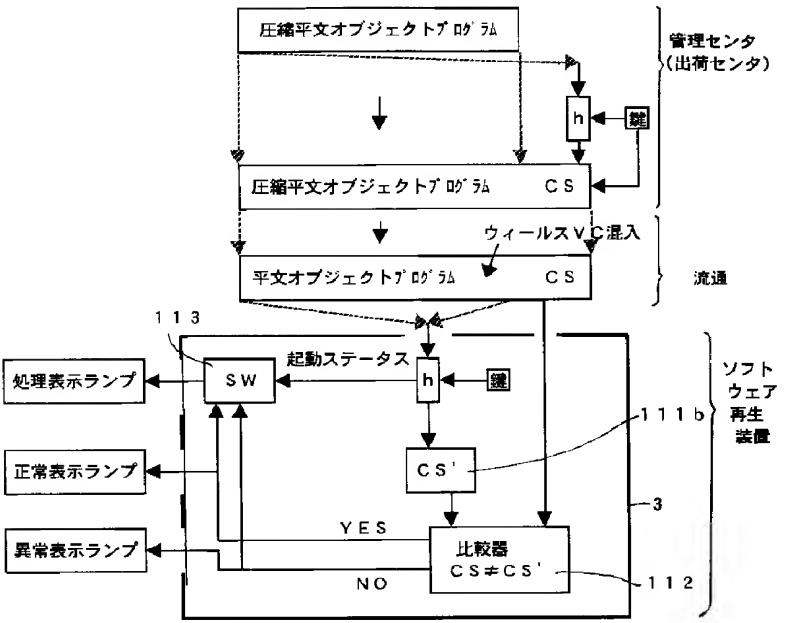


【図１３】

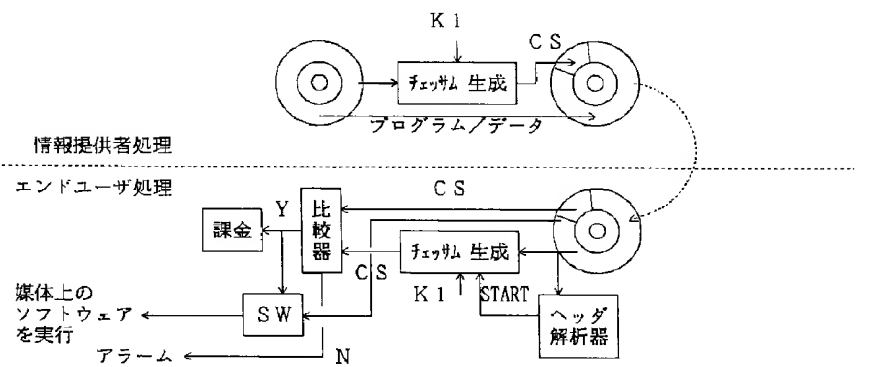


【図１０】

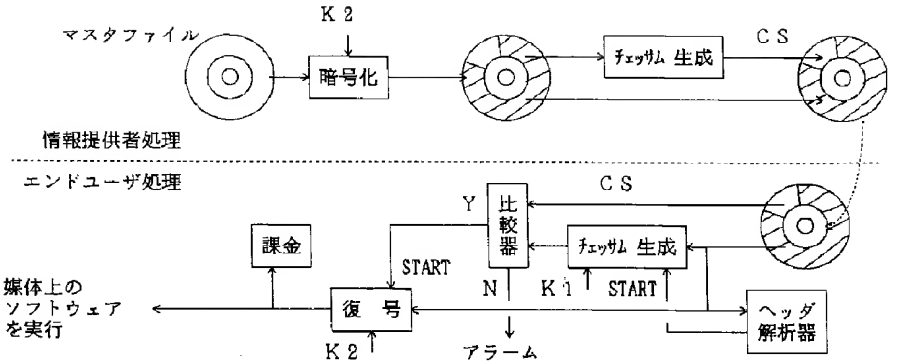
実施例において再生されるソフトウエアデータの完全性保証を確認するためのデータの構成を示すブロック図



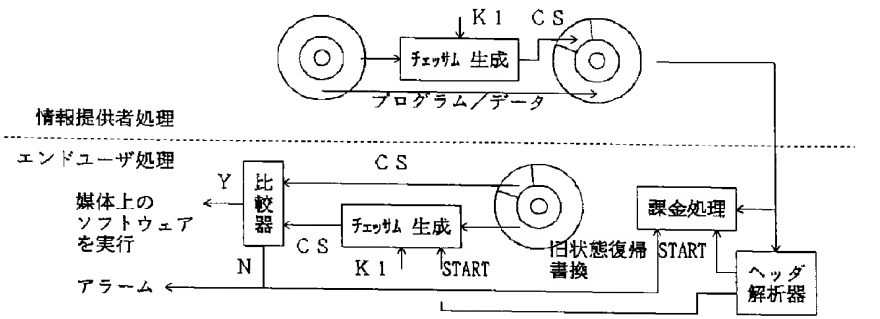
【図１４】



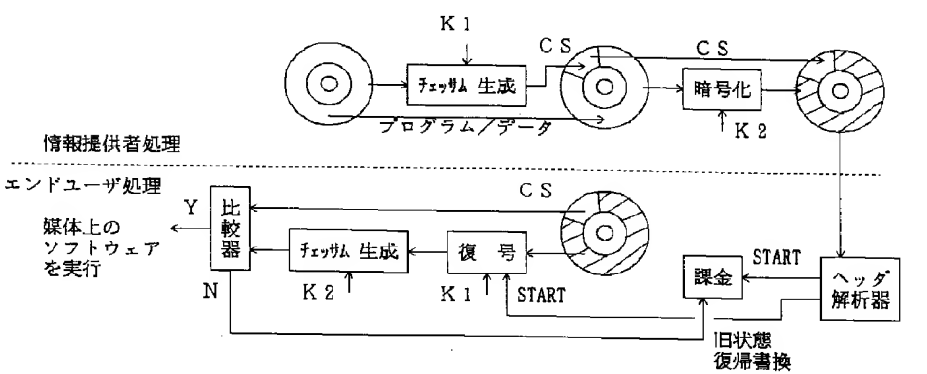
【図１５】


マスタファイル
Ｋ２
暗号化
チェッサム 生成
ＣＳ
情報提供者処理
エンドユーザ処理
Ｙ
比較器
ＣＳ
課金
チェッサム 生成
START
媒体上の
ソフトウェア
を実行
復　号
Ｎ
Ｋ１
START
ヘッダ
解析器
Ｋ２
アラーム

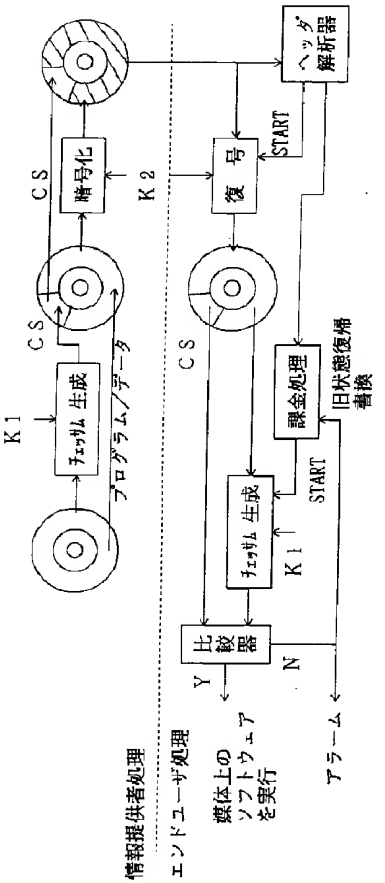
【図１７】


Ｋ１
ＣＳ
チェッサム 生成
プログラム／データ
情報提供者処理
エンドユーザ処理
ＣＳ
Ｙ
比較器
媒体上の
ソフトウェア
を実行
チェッサム 生成
課金処理
ＣＳ
旧状態復帰
書換
START
Ｎ
Ｋ１
START
ヘッダ
解析器
アラーム

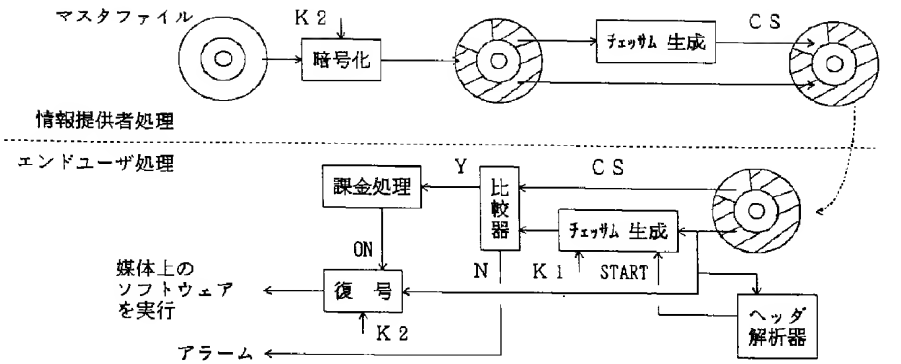
【図１９】


Ｋ１
ＣＳ
ＣＳ
チェッサム 生成
暗号化
プログラム／データ
Ｋ２
情報提供者処理
エンドユーザ処理
ＣＳ
Ｙ
比較器
媒体上の
ソフトウェア
を実行
チェッサム 生成
復　号
START
課金
ヘッダ
解析器
Ｎ
Ｋ２
Ｋ１
START
旧状態
復帰書換

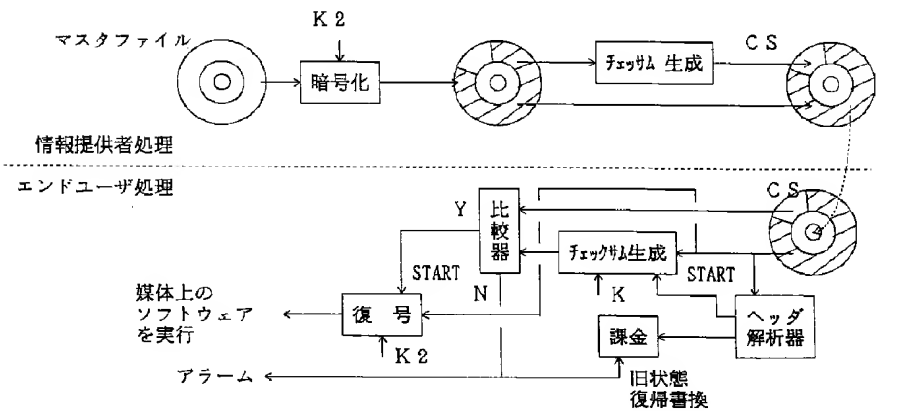
【図１６】


情報提供者処理
エンドユーザ処理
媒体上のソフトウェアを実行
アラーム
プログラム／データ
K1
K2
CS
暗号化
復号
ヘッダ解析器
START
課金処理
旧状態復帰書換
比較器
Y
N

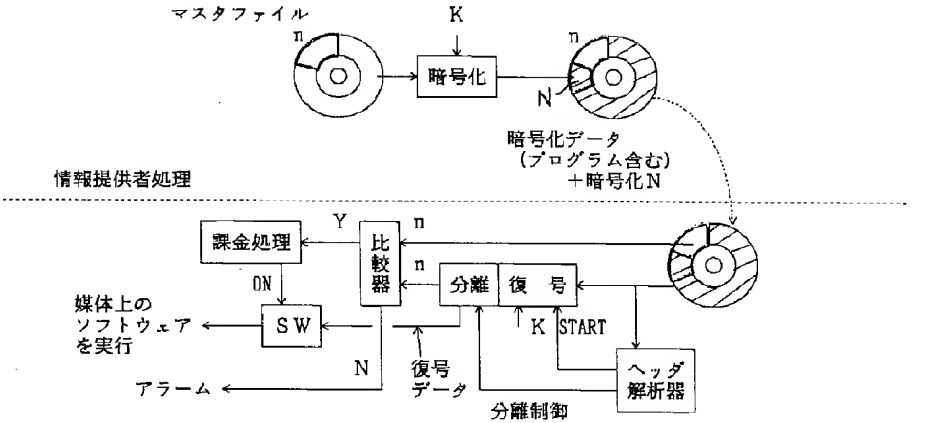
【図１８】


マスタファイル
K２
暗号化
ﾁｪｯｻﾑ 生成
ＣＳ
情報提供者処理
エンドユーザ処理
課金処理
Y
比較器
ＣＳ
ﾁｪｯｻﾑ 生成
ON
N
K１
START
媒体上のソフトウェアを実行
復　号
K２
ヘッダ解析器
アラーム

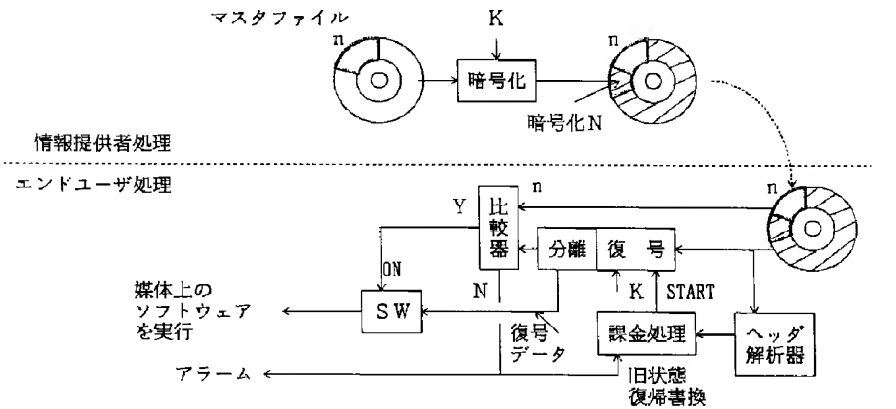
【図２０】


K２
マスタファイル
暗号化
ﾁｪｯｻﾑ 生成
ＣＳ
情報提供者処理
エンドユーザ処理
Y
比較器
ＣＳ
START
N
ﾁｪｯｸｻﾑ生成
START
K
媒体上のソフトウェアを実行
復　号
K２
課金
ヘッダ解析器
アラーム
旧状態復帰書換

【図２１】


マスタファイル
n
K
暗号化
n
N
暗号化データ
（プログラム含む）
＋暗号化N
情報提供者処理
課金処理
Y
比較器
n
n
分離
復　号
ON
媒体上の
ソフトウェア
を実行
SW
K
START
N
復号
データ
ヘッダ
解析器
アラーム
分離制御

【図２２】


マスタファイル
n
K
暗号化
n
暗号化N
情報提供者処理
エンドユーザ処理
Y
比較器
n
n
分離
復　号
ON
媒体上の
ソフトウェア
を実行
SW
N
K
START
復号
データ
課金処理
ヘッダ
解析器
アラーム
旧状態
復帰書換

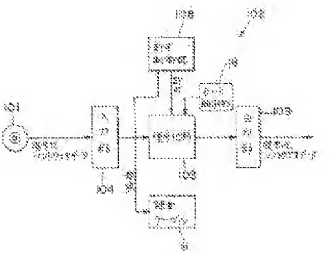
SOFTWARE MANAGEMENT MODULE AND SOFTWARE REPRODUCTION MANAGEMENT DEVICE/SYSTEM

Publication number: JP8106382 (A)
Publication date: 1996-04-23
Inventor(s): AKIYAMA RYOTA; YOSHIOKA MAKOTO
Applicant(s): FUJITSU LTD
Classification:
- international: ***G06F21/22; G06F1/00; G06F21/00; G09C1/00;*** **G06F21/22; G06F1/00; G06F21/00; G09C1/00;** (IPC1-7): G06F9/06; G09C1/00; G11B19/02
- European: G06F21/00N7P5H; G06F21/00N7D
Application number: JP19940225228 19940920
Priority number(s): JP19940225228 19940920; JP19940219372 19940810

Also published as:
JP3395863 (B2)
EP0702286 (A2)
EP0702286 (A3)
EP0702286 (B1)
US5737415 (A)

Abstract of **JP 8106382 (A)**

PURPOSE: To improve the security check efficiency and to attain the effective charging management without complicating the structure of a software storing medium by decoding the inputted ciphered software and then outputting this decoded software. CONSTITUTION: A decoding part 103 includes a mode indentification part 18 which consists of a DES and is controlled by a permission control part 108 to select the optimum one of various decoding modes in response to the software characteristic. The part 108 refers to a charging table 8 and permits the part 103 to perform a decoding processing job only when the charging balance is confirmed. Then the part 108 carries out the imposing a charge at a rate per unit of quantity to the table 8 in response to the reproduction of software and also informs an output part 109 of a fact that the charging balance is zero.; Thus both parts 108 and 103 are included in a module that is loaded into a software reproduction device so that the software charging is attained with high security.



Data supplied from the ***esp@cenet*** database — Worldwide